

FILED

AO 106 (Rev. 04/10) Application for a Search Warrant

AUTHORIZED AND APPROVED DATE



UNITED STATES DISTRICT COURT

for the
Western District of Oklahoma

4:11 pm, May 30, 2024

JOAN KANE, CLERK
U.S. DIST. COURT, WESTERN DIST. OKLA
By: RB, Deputy Clerk

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
A cellular telephone associated to phone number
405-412-6784, (IMEI# 35388566600880), to be seized
from Jose Manuel Granados Garcia and currently
located in the Western District of Oklahoma

Case No. M-24-482 -AMG

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A.

located in the Western District District of Oklahoma, there is now concealed (identify the person or describe the property to be seized):

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| Code Section | Offense Description |
|------------------------------|---|
| 18 U.S.C. §§ 922(a)(6) & 371 | Conspiracy to Make a False Statement During the Purchase of a Firearm |
| 18 U.S.C. § 933 | Trafficking Firearms |

The application is based on these facts:

See affidavit of ATF Special Agent Bryce Loesing.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Bryce A. Loesing
Applicant's signature

BRYCE LOESING, SPECIAL AGENT, ATF
Printed name and title

Sworn to before me and signed in my presence.

Date: 5/30/24

City and state: Oklahoma City, Oklahoma

Amanda Maxfield Green
Judge's signature

AMANDA MAXFIELD GREEN, U.S. Magistrate Judge
Printed name and title

**IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF OKLAHOMA**

**A Cellular Telephone Associated
to Phone Number 405-412-6784,
(IMEI# 353885666600880), to be
seized from Jose Manuel
Granados Garcia and currently
located in the Western District of
Oklahoma.**

Case No. M-24- -AMG

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Bryce Loesing, being duly sworn, depose and state as follows:

1. I have been employed as a Special Agent with the United States Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) since May of 2022. Prior to my employment with ATF, I was employed by the Wichita Police Department in Wichita, Kansas, for approximately 8 years. I am a graduate of the Federal Law Enforcement Training Center and the ATF National Academy and am currently assigned to the Oklahoma City Field Office. As a Special Agent with ATF, I investigate violations of Federal Law, including violations of the Gun Control Act of 1968, as amended (Title 18, United States Code, Sections 921 et seq.), and explosives, arson, alcohol, and tobacco laws. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants under the authority of the United States.

2. I am currently investigating **Jose Manuel Granados Garcia (GARCIA)** (DOB: XX/XX/1992) for, *inter alia*, conspiring to make a false statement during the purchase of a firearm in violation of 18 U.S.C. §§ 922(a)(6) and 371, and trafficking firearms in violation 18 U.S.C. § 933. I am submitting this Affidavit in support of a search warrant authorizing a search of **GARCIA's** cellular telephone: an unknown model, phone number +1 (405) 412-6784, IMEI# 353885666600880 (hereinafter **SUBJECT PHONE**), as further described in **Attachment A**, which is incorporated into this Affidavit by reference. The **SUBJECT PHONE** is currently in **GARCIA's** possession. I am submitting this Affidavit in support of a search warrant authorizing a search of the **SUBJECT PHONE** for the items specified in **Attachment B** hereto, wherever they may be found, and to seize all items in **Attachment B** as instrumentalities, fruits, and evidence of the aforementioned crime.

3. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me regarding this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant. The information contained in this Affidavit is based upon my personal knowledge and observation, my training and experience,

conversations with witnesses and other law enforcement officers, and my review of documents and records.

PROBABLE CAUSE

4. On May 7, 2024, I received information from the ATF Field Office in Austin, Texas, indicating that GARCIA had instructed two individuals, PEDRO CASTILLO JR. and ANGEL DE LA CRUZ, to purchase firearms from a Federal Firearms Licensee (FFL) in Austin, Texas, and ship the firearms to Oklahoma City, Oklahoma, so that GARCIA could receive them.

5. On May 10, 2024, I conducted an in-person interview with CASTILLO who admitted that GARCIA had asked him to purchase two firearms on GARCIA's behalf. CASTILLO informed me that GARCIA had given him instructions as to which firearms to buy, where to have them shipped, and how to transfer them to GARCIA. CASTILLO confirmed that he had ordered just one of the firearms requested by GARCIA because it was the only one for sale at the time. CASTILLO confessed that GARCIA had given him \$9,500 in cash to pay for the firearm; and \$2,000 in cash as payment for making the straw purchase. With CASTILLO's consent, I was able to review text messages between CASTILLO and GARCIA on CASTILLO's phone—my review of those messages confirmed CASTILLO's account.

6. On April 15, 2024, GARCIA sent CASTILLO a link to "elitefirearmsonline.com" via text message. GARCIA also sent CASTILLO

text messages stating: "M82a1"; "Get 2 day shipping"; "Get it shipped to h&h I think there ffl transfer fee 50"; "This week if u can si no I need for sure before next Saturday."

7. On April 16, 2024, CASTILLO and GARCIA exchanged the following text messages:

GARCIA: "I'll buy some time."

CASTILLO: "I tried and look back at the other one and still nothing."

GARCIA: "Or lemme see if I can find one tonight."

CASTILLO: "Ooooh" "Bet" "Almost ordered it."

GARCIA: "Go ahead bro fuck it" . . . "[w]ith proof it's been ordered they'll wait."

8. On April 18, 2024, GARCIA sent CASTILLO a text message stating "I gave you 10k plus 1000 for u. I found the paper where I wrote it down."

9. On April 19, 2024, GARCIA and CASTILLO discussed, via text message, CASTILLO ordering an FN M249s Standard SAW firearm from Kygunco.com, which is based in the state of Kentucky. GARCIA instructed CASTILLO to pay for two-day shipping. The conversation continued via text messages through April 23, 2024, when GARCIA and CASTILLO discussed meeting in person to exchange an "item," which CASTILLO told me was a firearm, that CASTILLO picked up on that day.

10. On May 21, 2024, I received an ATF Form 4473 ("the 4473 Form") from H & H Shooting Sports at 400 Vermont Ave., Oklahoma City, Oklahoma. The 4473 Form was completed by CASTILLO on April 23, 2024, at H & H. In box 21, sub section "a," on the 4473 Form, which asks "Are you the actual transferee/buyer of all of the firearm(s) listed on this form and any continuation sheet(s)...?", CASTILLO indicated that he was actual transferee/buyer by marking the "Yes" box with an "x."

11. On May 21, 2024, I conducted a second in-person interview with CASTILLO. CASTILLO admitted that he ordered the firearm listed on the 4473 Form for GARCIA. CASTILLO confirmed that GARCIA gave him cash to pay for the firearm as well as cash to keep for making the purchase. CASTILLO admitted to going to H & H on April 23, 2024, completing the 4473 Form, picking up the firearm, and turning the firearm over to GARCIA in the area of H & H immediately thereafter.

12. CASTILLO admitted that he had marked on the 4473 Form that he was the actual transferee/ buyer, but that he was actually purchasing the firearm on behalf of GARCIA.

13. CASTILLO showed me the listed contact phone number for "Jose" (GARCIA) in his cell phone. I was able to confirm that the aforementioned communications were between CASTILLO's phone and the SUBJECT PHONE based on the phone numbers.

14. On May 24, 2024, I served T-Mobile US, Inc. with a Grand Jury Subpoena for all records related to **GARCIA**, the address 3729 N Shannon Ave., Bethany, Oklahoma 73008, and phone number +1 (405) 412-6784.

15. On May 29, 2024, the records were returned to me by T-Mobile US, Inc. The records named Maria Granados (DOB XX/XX/2000), as the subscriber of the **SUBJECT PHONE**, with an activation date of February 20, 2023. The subscriber address was listed as 3004 SW 28th St, Oklahoma City, Oklahoma 73108. Call Detail Records confirmed contact between the **SUBJECT PHONE** and **CASTILLO's** phone, +1 (405) 650-8906.

16. Oklahoma Driver's License records identify Maria Granados as Maria Guadalupe Granados Garcia with the same date of birth as the subscriber of the **SUBJECT PHONE**.

17. Maria Guadalupe Granados Garcia is believed to be a member of **GARCIA's** immediate family based on vehicle registration records showing both individuals with vehicles currently registered at the same address.

18. Based on my training and experience, I am aware that individuals involved in trafficking firearms often use straw purchasers to conceal their identity. Those individuals usually use cell phones to maintain contact with other co-conspirators, including straw purchasers, transporters, and purchasers of illegally trafficked firearms. Such cell phones and their associated memory cards commonly contain electronically stored information

which constitutes evidence, fruits, and instrumentalities of firearm trafficking offenses including, but not limited to, the phone directory and/or contacts list, calendar, text messages, e-mail messages, call logs, photographs, and videos.

BIOMETRIC ACCESS TO DEVICES

19. I request that this warrant permit law enforcement to compel **GARCIA** to unlock any electronic devices requiring biometric access subject to seizure pursuant to this warrant. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple has offered a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the

relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face.

The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this Affidavit, I have reason to believe that **GARCIA** is in possession of a cellular telephone (**SUBJECT PHONE**). The passcode or password that would unlock the **SUBJECT PHONE** to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the electronic devices, making the use of biometric

features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, certain Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for eight hours and the passcode or password has not been entered in the last six days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter the **SUBJECT PHONE**, and it may be unlocked using one of the aforementioned biometric features, this warrant permits law


enforcement personnel to: (1) press or swipe the fingers (including thumbs) of **GARCIA** to the fingerprint scanner of the **SUBJECT PHONE**; (2) hold the **SUBJECT PHONE** in front of the face of **GARCIA** and activate the facial recognition feature; and/or (3) hold the **SUBJECT PHONE** in front of the face of **GARCIA** and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant. The proposed warrant does not authorize law enforcement to require that **GARCIA** state or otherwise provide the password or any other means that may be used to unlock or access the devices. Moreover, the proposed warrant does not authorize law enforcement to require **GARCIA** to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access the devices.

CONCLUSION


Based on the above information, I submit that there is probable cause to believe that violations of 18 U.S.C. §§ 922(a)(6) and 371 have occurred, and that evidence, fruits, and instrumentalities of these offenses and 18 U.S.C. § 933 are located on the **SUBJECT PHONE**. Therefore, I respectfully request that this Court issue a search warrant for the **SUBJECT PHONE**, described

in Attachment A, authorizing the seizure of the items described in Attachment B.

Respectfully submitted,


BRYCE LOESING
Special Agent
Bureau of Alcohol, Tobacco,
Firearms and Explosives

SUBSCRIBED AND SWORN to before me this 30th day of May 2024.


AMANDA MAXFIELD GREEN
United States Magistrate Judge

ATTACHMENT A

The property to be searched is an unknown model cellular telephone, phone number +1 (405) 412-6784, IMEI# 353885666600880; SIM: 8901260560774331432; and IMSI: 310260567433143 (hereinafter **SUBJECT PHONE**). The **SUBJECT PHONE** is currently in the possession of **GARCIA** who is believed to be located in the Western District of Oklahoma.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, ATF may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

1. All records on the **SUBJECT PHONE**, described in Attachment A, that relate to violations of 18 U.S.C. §§ 922(a)(6), 371, and 933 that involve **GARCIA** including:

- a. any information recording **GARCIA**'s schedule or travel;
- b. any text messages, instant messages, or electronic messages communicating between known or unknown co-conspirators;
- c. any photos of stolen items;
- d. any photos of firearms;
- e. any phone records between known or unknown co-conspirators;
- f. lists of customers and related identifying information including images and videos;
- g. types, quantity, and prices of firearms that were purchased by straw purchasers and/or trafficked as well as dates, places, and amounts of specific transactions;
- h. any information related to the sources of firearms, including: names, addresses, phone numbers, or any other identifying information;

i. all bank records, checks, credit card bills, account information, and other financial records;

j. all communications between **GARCIA, PEDRO CASTILLO JR.**, and **ANGEL DE LA CRUZ**;

k. evidence of user attribution showing who used or owned the **SUBJECT PHONE** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

- i. records of Internet Protocol addresses used;
- ii. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records” and “information” include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored on the **SUBJECT PHONE**.